AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[redacted]

Case No. B-18-1119-MJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: [redacted]

See attachment C

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252A(a)(5)(B)	knowingly possesses or knowingly accesses with intent to view any material that contains an image of child pornography using any means or facility of interstate or foreign commerce by any means, including by computer.

The application is based on these facts:

See attachment A

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[signature]
Applicant's signature

Scott McIver, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/26/2018

[signature]
Judge's signature

City and state: Brownsville, Texas

Ignacio Torteya, III - U.S. Magistrate Judge
Printed name and title

B-18-1119-MJ

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF TEXAS

IN THE MATTER OF THE SEARCH OF:

The residential property located at:
[redacted]

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT
ATTACHMENT A

I, Scott P. McIver, being duly sworn, depose and say that:

1. I am a Special Agent with the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been a Special Agent since September 2017. I graduated from the Criminal Investigator Training Program (CITP) and Homeland Security Investigations Special Agent Training (HSISAT) programs at the Federal Law Enforcement Training Center (FLETC) in Glynco, GA. Prior to becoming a Special Agent with HSI, my previous law enforcement experience consists of 13 years (2004 to 2017) working as a Police Officer, Deputy Sheriff, and State Agent with agencies in the Lafayette, Louisiana area and statewide, to include the Lafayette City Police Department, the Lafayette Parish Sheriff's Office, and the Louisiana Alcohol and Tobacco Control Enforcement Division.

2. As part of my official duties, I have conducted and participated in investigations relating to the sexual exploitation of children. During these investigations, I have observed and reviewed examples of child pornography in various forms of media, including computer media. I have also received training and instruction in the field of investigating child pornography.

3. This affidavit is being submitted in support of an Application for a Search Warrant for a residential home, freestanding structures, and vehicles located at [redacted] (hereinafter TARGET RESIDENCE). Photographs of residence are contained in Attachment C to this Affidavit. The search is for any computer hardware therein, for evidence of violations of Title 18, United States Code, Section 2252A(a)(5)(B) and Title 18, United States Code, Section 2252A(a)(2), entitled "Certain activities relating to material constituting or containing child pornography."

4. Based upon the information summarized in this application, I have reason to believe that evidence of such violations is located at the named residential property.

5. The statements in this Affidavit are based in part on my investigation of this matter, and information provided to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact of this investigation.

APPLICABLE LAW

6. This investigation concerns alleged violations of Title 18, United States Code, Section 2252A(a)(5)(B) and Title 18, United States Code, Section 2252A(a)(2), relating to the possession and distribution of child pornography.

7. Title 18, United States Code, Section 2252A(a)(5)(B) prohibits any person from knowingly possessing, or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. Title 18, United States Code, Section 2252A(a)(2) prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer. Title 18, United States Code, Section 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

9. Per Title 18, United States Code, Section 2256(1), the term "minor" means any person under the age of eighteen years.

10. Per Title 18, United States Code, Section 2256(8), the term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

11. Per Title 18, United States Code, Section 2256(2)(A), except as provided in subparagraph B, "sexually explicit conduct" means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition of the genitals or pubic area of any person.

12. For purposes of subsection 8(B) of this section, "sexually explicit conduct" means graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; graphic or lascivious simulated bestiality, masturbation, sadistic or masochistic abuse; or graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

CHILD PORNOGRAPHY ON THE INTERNET

13. Pursuant to your Affiant's training and experience, as well as the training and experience of other law enforcement personnel, your Affiant has learned that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contacts with other individuals who have it available. The use of the internet to traffic in, trade, or collect child pornography has become one of the preferred methods of obtaining this material. An individual familiar with the internet can use it, usually in the privacy of his own home, to interact with another individual or a business offering such materials. The use of the internet offers individuals interested in obtaining child pornography a sense of privacy and secrecy not available elsewhere.

14. Based upon your Affiant's training and experience, your Affiant knows the internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the internet. The World Wide Web (www) is a functionality of the internet, which allows users of the internet to share information.

15. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods. Child pornography obtained via the internet can be saved to a variety of electronic media, including hard disk drives, flash memory devices, CDs, DVDs, and others.

COMPUTER TERMS

16. For the purposes of this affidavit, unless otherwise specifically indicated, the term computer, as defined in 18 USC §1030(e) (1), refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communication devices (such as internal modems capable of sending/receiving electronic mail or fax cards) along with any other hardware stored or housed internally. Printers, external modems (attached by cable to the main unit), monitors and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term computer system is used. Information refers to all the information on a computer system including both software applications and data.

17. The term computer hardware as used in this affidavit refers to all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, memory typewriters, and self-contained laptops or notebook computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone generating devices); as well as

any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

18. The term computer software as used in this affidavit refers to digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters and communications programs.

19. The term computer-related documentation used in this affidavit refers to written, recorded, printed or electronically stored material, which explains or illustrates how to configure or use computer hardware, software or other related items.

20. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric or other special characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby- trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

21. Visual depictions in the computer environment are usually in the form of "computer graphic files." Computer graphic files are files where photographs have been digitized into computer binary format. Once in this format the graphic file can be viewed, copied, stored, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Common types of computer graphic image files encountered are those in a Joint Photographic Experts Group or JPEG format having the ".jpg" file extension, those graphic files in a Graphic Interchange Format or GIF having the ".gif" file extension, and those graphic files in a Tagged Image File format or TIF having the ".tif" file extension. Common video files encountered are those in a Moving Picture Experts Group or MPEG format having the ".mpeg" or ".mpg" file extension and the Audio Video Interleave or AVI format having the ".avi" file extension. Although other file formats exist, these are the most common formats encountered.

COMPUTER SEARCHES

22. Based on your Affiant's consultation with experts in computer searches, data retrieval from computers and related media, and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems, as well as your Affiant's own training and experience, your Affiant knows that searching computerized information for evidence and instrumentalities of a crime requires the seizure of all input/output peripheral devices, device-related software (including passwords), documentation, and data security so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. These searches can be complex and time consuming. This is true because of the following:

23. Computer storage devices (like hard disks, diskettes, tapes, laser disks, CD- ROMs, and DVDs) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may

try to conceal criminal evidence, and he might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks, depending on the volume of data stored, and it would be impractical to attempt this kind of thorough data search on site.

24. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

25. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of available computer hardware and software requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and / or from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

26. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and/or data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable time.

27. Investigations have shown that the computer and its storage devices, the monitor, keyboard, and modem can all be instrumentalities of the crime of advertising, distribution, receipt, and/or possession of child pornography in violation of law, and should all be seized as such.

28. In your Affiant's experience and after consultations with other agents and experts in the field of child exploitation who have been involved in investigations related to child pornography, it is of great value during a search to secure all photographs of children, regardless of whether or not the photographs meet the definitions of child pornography, in that the photographs are crucial in identifying any victims of child pornography whose images may be contained in law enforcement repositories of victims of child pornography.

PEER TO PEER FILE SHARING AND THE BITTORRENT NETWORK

29. Peer-to-Peer (P2P) file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the internet. Peer-to-Peer file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files. Peer-to-Peer file sharing networks, such as the BitTorrent Network are frequently used to trade image and video files of child pornography.

30. Based on my knowledge and experience, this Affiant has learned the following regarding the operation of the BitTorrent file-sharing network:

30(a). BitTorrent is an open source public file-sharing network. Most computers that are part of this network are referred to as peers or hosts. A peer can simultaneously provide files to peers while downloading files from other peers. Peers may be elevated to temporary indexing servers referred to as an "ultra-peer." Ultra-peers increase the efficiency of the BitTorrent network by maintaining an index of the contents of network peers. BitTorrent users query ultra-peers for files and are directed to one or more peers sharing that file. There are many ultra-peers on the network, if one shuts down the network continues to operate.

30(b). The BitTorrent network can be accessed by computers running many different client programs. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client.

30(c). During the default installation of a BitTorrent client, settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

30(d). Typically, a "setting" establishes the location of one or more directories or folders whose contents (files) are made available for distribution to other BitTorrent peers.

30(e). Typically, a "setting" controls if other users of the network can obtain a list of the files being shared by the host computer.

30(f). Typically, a "setting" controls if users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

30(g). Files located in a peer's shared directory are processed by the client software. As part of this processing, a SHA1 hash value is computed for each file in the user's shared directory.

30(h). A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide certainty that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

30(i). The BitTorrent network uses SHA1 values to improve network Efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple peers and then

reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA1 values to ensure exact copies of the same file are used during this process.

30(j). Upon connecting to the BitTorrent network, the BitTorrent client compiles a list of the shared files, files details and the file's associated SHA1 values and submits the list to the ultra-peers. This information is then propagated to other ultra-peers throughout the network. The frequency of updating information as file changes occur or candidates leave the network is dependent upon the client software being used and networking protocols. The information sent to the ultra-peers is data about the file and not the actual file. The file remains on the peer computer. In this capacity, the ultra-peer acts as a pointer to the files located on each peer. The network may be referred to as decentralized due in part to the fact that files do not reside on a single server but are located on individual peers throughout the network.

30(k). The BitTorrent software allows the user to search for pictures, movies and other files by entering descriptive text as search terms. These terms are typically processed by the ultra-peers based upon the information about the files that had been sent by individual peers.

30(l). Entering search terms into a BitTorrent client returns a list of files and descriptive information including, in some client software, the associated SHA1 signature.

30(m). A person can compare the SHA1 signatures of files being shared on the network to previously identified SHA1 signatures of any file including child pornography. Using a publicly available BitTorrent client a user can select the SHA1 signature of a known file and attempt to receive it.

30(n). Once a specific file is identified, the download process can be initiated. Once initiated, a user is presented with a list of peers or IP addresses that have recently been identified as download candidates for that file. This allows for the detection and investigation of computers involved in possessing, receiving and/or distributing files of previously identified child pornography.

30(o). The IP addresses can be used to identify the location of these computers. A review of the SHA1 signatures allows an investigator to identify the files that are child pornography.

30(p). The returned list of IP addresses can include computers that are likely to be within this jurisdiction. The ability to identify the approximate location of these IP address is provided by IP geographic mapping services, which are publicly available and used for marketing and fraud detection. At this point in the investigative process, a recent association between a known file (based upon SHA1 comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

30(q). Once this association has been established, an investigator can attempt to download the file from the associated peer or view the contents of the shared directory. Depending upon several factors including configuration and available resources, it might not be possible to do either.

30(r). Depending on the associated peer configuration and available peer resources a listing of the files being shared may be displayed. The file list can only be obtained if the associated peer is connected to the network and running a BitTorrent client at that moment.

30(s). By receiving either a file list or portions of a download from a specific IP address the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent client and possessing, receiving and/or distributing specific and known visual depictions of child pornography.

DETAILS OF THE INVESTIGATION

31. On or about May 9, 2018, special agents from the Rio Grande Valley Child Exploitation Investigation Task Force (RGV CEITF) conducted an online investigation on the BitTorrent network for offenders sharing child pornography on the internet. Internet Protocol (IP) address 70.117.196.153 was identified as possessing and distributing child pornography. Using a computer running investigative BitTorrent software, agents monitored IP address 70.117.196.153.

32. During the investigation agents conducted a search of IP address 70.117.196.153 using a website established by law enforcement for child exploitation investigations. The website is used to share information on IP addresses suspected of possessing and distributing child pornography and for deconfliction purposes. The website is affiliated with Internet Crimes Against Children (ICAC) program. The ICAC program is a nationwide initiative comprised of law enforcement personnel from federal, state and local law enforcement established to combat the exploitation of children on the internet.

33. RGV CEITF agents successfully downloaded numerous friles that the device at IP address 70.117.196.153 was making available. The device at IP address 70.117.196.153 was the sole candidate for each download, and as such, each file was downloaded directly from this IP address.

34. Two video/image files were selected as a representative sample for this affidavit to establish these files do in fact contain child pornography. The following is a sample description of the files possessed and distributed by the user at IP address 70.117.196.153:

34(a). The first file is a video approximately fifty-six (56) seconds in length. The video file depicts a prepubescent minor female disrobing, masturbating, then posing for the camera.

34(b). The second file is a video approximately eight (8) minutes and forty-four (44) seconds in length. The video file depicts a minor female disrobing and posing for the camera as she rubs her body. Later in the video, an adult male hand comes into view and begins rubbing the minor female's vagina. The video continues with the female changing positions as she masturbates and the male's hand rubs the minor female's buttocks. The adult male also inserts his finger into the minor female's vagina several times throughout the video. The video ends with the minor female blowing a kiss to the camera.

35. On May 9, 2018, agents conducted a query on the IP address 70.117.196.153 through the American Registry for Internet Numbers (ARIN). ARIN reported IP address 70.117.196.153 to be registered to Time Warner Cable Internet LLC.

36. On May 16, 2018, SA McIver served and received a summons return from Time Warner Cable (Charter Communications, Inc.) for subscriber information for IP address 70.117.196.153. The subscriber information returned by Time Warner Cable (Charter Communications, Inc.) is as follows:

Subscriber Name: Juan ESPINOSA

Subscriber Address: [redacted]
MAC: 40490fc3069d
Phone Number: ([redacted]

37. The TARGET RESIDENCE is a single-story home located in San Juan, Texas. The home is a brick style construction, tan in color, with a white front door. The numbers [redacted]" are displayed on a tan, brick mailbox near the end of the driveway and on the home near the front door. The driveway of the home is in the front of the house, accessed via [redacted]. The investigation has also revealed that the home does not have an open WiFi.

38. The investigation revealed that Bertha Franco-Vitela (DOB [redacted]/1963) and Ernesto Franco (DOB [redacted]/1995) are the primary residents of the TARGET RESIDENCE, and Bertha Franco-Vitela has an associated phone number of [redacted], which is consistent with the Time Warner Cable (Charter Communications, Inc.) subscriber for the TARGET RESIDENCE. Juan ESPINOSA's Texas identification card also identifies "Bertha Vitela" and "Bertha Franco" as an emergency contact.

39. On July 27, 2018, SA McIver received a summons return from Time Warner Cable (Charter Communications, Inc.) that showed a new IP address associated with the TARGET RESIDENCE, but the subscriber information remained the same. Further investigation revealed that the new IP address (72.178.176.40) had multiple child pornography downloads associated with it.

40. As of October 18, 2018, at 05:07:37 AM (UTC), hash values associated with known child pornography were found while monitoring IP address 72.178.176.40.

CHILD PORNOGRAPHY COLLECTION

41. Based upon your Affiant's training and experience, and after consulting with other investigators working these matters, your Affiant has learned that child pornography distributors/collectors:

41(a). Receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs or other visual media) or from literature describing such activity.

41(b). Collect sexually explicit or suggestive materials (hard-core and soft-core pornography) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, they may use this type of sexually explicit material to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, and to demonstrate the desired sexual acts.

41(c). Almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, security of pornography, "child erotica," etc.) in the privacy of their homes or some other secure location. Child distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

41(d). Often correspond and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, including email addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

41(e). Generally, prefer not to be without their child pornography and/or child erotica for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

41(f). Maintain their collections in a safe, secure environment such as a home computer and surrounding area, because this material is illegal, can be difficult to obtain, and can be difficult to replace. These collections are maintained for extended periods of time, if not indefinitely, and are kept close by, usually at their residence to enable the collector to view his collection which he values highly.

42. The visual images obtained, traded, and/or sold are prized by child pornography collectors, and have emotional value to the collector. The visual images are intrinsically valuable for trading or selling and therefore are destroyed or deleted only rarely by the collector. These images are often maintained by the offender to blackmail the victim in the future, if necessary.

43. Kenneth V. Lanning is a retired FBI agent and a widely acknowledged expert in the field of child sexual exploitation. Lanning spent 30 years with the FBI's Behavioral Science Unit in Quantico, VA, and in 1997 he received the FBI Director's Award for Special Achievement for his career accomplishments in connection with missing and exploited children. Lanning has aptly noted that many collectors of child pornography swap pornographic images the way children swap baseball cards and that preferential sex offenders with a sexual preference for children tend to collect predominately child pornography or erotica. They typically collect things such as books, magazines, articles, newspapers, photographs, negatives, slides, movies, albums, digital images, drawings, audiotapes, video recordings and equipment, personal letters, diaries, clothing, sexual aids, souvenirs, toys, games, lists, paintings, ledgers, and photographic and computer equipment all relating to their preferences and interests in a sexual, scientific, or social way. It is also common for pedophiles to record their contacts and sexual abuse of children. These collections and records are so important to pedophiles that they tend to keep them for extended periods of time, often years. Lanning has found, moreover, that no matter how much child pornography the collector has, he never seems to have enough, and he rarely throws anything away. Another typical feature of a child pornography collection, according to Lanning, is its constancy. Even if evidence of the existence of child pornography is several years old, Lanning states: "chances are [the preferential sex offender] still has the collection now – only it is larger." (Child Molesters: A Behavioral Analysis, by Kenneth V. Lanning, Fifth Edition, Pub. 2010, by the National Center for Missing & Exploited Children.) In addition, your Affiant's experience and training has shown that such material is normally and generally kept in the individual's office, residence, automobile, or other secure location to ensure convenient and ready access.

APPLICATION

44. Based on the information, your Affiant respectfully submits that there is probable cause to believe that Juan A. ESPINOSA, who is believed to reside at the TARGET RESIDENCE, depicted in the photograph attached as Attachment C to this Affidavit, is involved in the possession and distribution of visual depictions of minors engaged in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce in violation of Title 18 U.S.C. Sections 2252A(a)(5)(B) and 2252A(a)(2). Additionally, there is probable cause to believe that evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. Sections 2252A(a)(5)(B) and 2252A(a)(2) is located in the residence or structures photographed in Attachment C to this Affidavit or vehicles parked at the TARGET RESIDENCE, and in computer hardware therein, and this evidence which is listed in Attachment B to this Affidavit, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

45. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of all electronic storage media located during the search of the TARGET RESIDENCE, vehicles, and any free-standing structures located at the TARGET RESIDENCE.

Scott P. McIver
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 26th day of November 2018.

IGNACIO TORTEYA, III
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED, SEIZED AND EXAMINED

This affidavit is in support of application for a warrant to search the above mentioned computers and peripherals, which are more specifically identified in the body of the application, including any computers, associated storage devices and/or other devices located therein that can be used to store information and/or connect to the Internet, for records and materials evidencing a violation of Title 18, United States Code, Sections 2252 and 2252A, which criminalizes, in part, the possession, receipt and transmission of child pornography (defined in Title 18, United States Code, Section 2256), as more specifically identified below:

1. Any and all computers, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, tape systems and hard drive, terminals (keyboards and display screens) and other computer related operation equipment, in addition to computer photographs, digital graphic file formats and/or photographs, slides or other visual depictions of such digital graphic file format equipment that may be used to visually depict child pornography, child erotica, information pertaining to the sexual interest in child pornography, sexual activity with children or the distribution, possession, or receipt of child pornography, child erotica or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.

4. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

5. In any format and media, all originals, copies and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or child erotica.

6. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages) identifying persons transmitting through interstate or foreign commerce, including via computer, any visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or child erotica.

7. Any and all records and materials, in any format and media (including, but not limited to, envelopes, letters, papers, e-mail, chat logs, electronic messages, other digital data files and web cache information), bearing on the receipt, shipment or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

8. Records of communication (as might be found, for example, in digital data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or who cater to those with an interest in child pornography, as well as evidence of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.

9. Evidence of association, by use, subscription or free membership, with online clubs, groups, services or other Internet sites that provide or otherwise make accessible child pornography.

10. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.

11. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

12. Records, in any format or media, evidencing ownership or use of computer equipment and paraphernalia found in the residence to be searched, including, but not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, handwritten notes and handwritten notes in computer manuals.

13. Graphic files (including, but not limited to files bearing graphic interchange format extensions, .JPG, .GIF, .TIF, .AVI and .MPG), and the data within the aforesaid objects relating to said materials, which may be, or are, used to visually depict child pornography or child erotica.

14. Any and all computer programs capable of viewing graphic files.

15. Names and addresses of minors visually depicted while engaged in sexually explicit conduct.

16. Files depicting sexual conduct between adults and minors.

17. Any and all records evidencing use or ownership of the computer described above, including, but not limited to, registry and setup information within the computer's operating system and customization to the operating system's directory structure.

18. Any and all photographs, compact disks, DVDs, motion picture films (including but not limited to 8mm film), super 8 video, video cassette tapes, production and reproduction equipment, motion picture cameras, video cameras, video cassette recorders, and other photographic and video recording equipment used to produce or reproduce photographs, motion picture films, or video cassettes, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence

a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct.

19. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.

20. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential/business premises described as and items contained therein, computer equipment, accessories, telephone(s), modems(s) or such records, whether stored on paper, in files, invoices, bills, leases deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, or storage media.

21. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.

22. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access relating to any internet service provider, all handwritten notes and handwritten notes in computer manuals.

23. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers of facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of child pornography.

24. All software, manuals, documents or records relating to the operation of file servers.

ATTACHMENT C

[redacted]

The residence is a single-story home located in San Juan, Texas. The home is a brick style construction, tan in color, with a white front door. The numbers [redacted]' are displayed on a tan, brick mailbox near the end of the driveway and on the home near the front door. The driveway of the home is in the front of the house, accessed via Calle Tulipan.